physical form or characteristics, that is owned by, produced by or for, or under the control of the United States Government, and determined pursuant to Executive Order 12356, April 2, 1982 (47 FR 14874, April 6, 1982) or prior orders to require protection against unauthorized disclosure, and is so designated.

[48 FR 42113, Sept. 19, 1983, as amended at 51 FR 2649, Jan. 17, 1986]

4.402 General.

(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled ''National Industrial Security Program'' (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960 (25 FR 1583, February 25, 1960), entitled ''Safeguarding Classified Information Within Industry,'' as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).

(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive Orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DOD publications implement the program:

(1) *National Industrial Security Program Operating Manual* (NISPOM) (DOD 5220.22–M).

(2) *Industrial Security Regulation* (ISR) (DOD 5220.22–R).

(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.

(d) Part 27, Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

[48 FR 42113, Sept. 19, 1983, as amended at 61 FR 31617, June 20, 1996]

4.403 Responsibilities of contracting officers.

(a) *Presolicitation phase.* Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor during contract performance.

(1) If access to classified information of another agency may be required, the contracting officer shall—

(i) Determine if the agency is covered by the NISP; and

(ii) Follow that agency's procedures for determining the security clearances of firms to be solicited.

(2) If the classified information required is from the contracting officer's agency, the contracting officer shall follow agency procedures.

(b) *Solicitation phase.* Contracting officers shall—

(1) Ensure that the classified acquisition is conducted as required by the NISP or agency procedures, as appropriate; and

(2) Include (i) an appropriate Security Requirements clause in the solicitation (see 4.404), and (ii) as appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause (52.204–2, Security Requirements).

(c) *Award phase.* Contracting officers shall inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract as follows:

(1) Agencies covered by the NISP shall use the Contract Security Classification Specification, DD Form 254. The contracting officer, or authorized representative, is the approving official for the form and shall ensure that it is prepared and distributed in accordance with the ISR.

(2) Contracting officers in agencies not covered by the NISP shall follow agency procedures.

[48 FR 42113, Sept. 19, 1983, as amended at 61 FR 31617, June 20, 1996]

4.404 Contract clause.

(a) The contracting officer shall insert the clause at 52.204–2, Security Requirements, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) below apply.

(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.

(c) If a construction or architect-engineer contract where employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II.

(d) If the contracting agency is not covered by the NISP and has prescribed a clause and alternates that are substantially the same as those at 52.204–2, the contracting officer shall use the agency-prescribed clause as required by agency procedures.

[48 FR 42113, Sept. 19, 1983, as amended at 61 FR 31617, June 20, 1996]

Subpart 4.5—Electronic Commerce in Contracting

SOURCE: 60 FR 34744, July 3, 1995, unless otherwise noted.

4.500 Scope of subpart.

This subpart provides policy and procedures for the establishment and use of the Federal Acquisition Computer Network (FACNET) as required by Section 30 of the Office of Federal Procurement Policy (OFPP) Act (41 U.S.C. 426).

4.501 Definitions.

ANSI X12, as used in this subpart, means the designation assigned by the American National Standards Institute (ANSI) for the structure, format, and content of electronic business transactions conducted through Electronic Data Interchange (EDI). ANSI is the coordinator and clearinghouse for national standards in the United States.

Electronic commerce (EC), as used in this subpart, means a paperless process including electronic mail, electronic bulletin boards, electronic funds transfer, electronic data interchange, and similar techniques for accomplishing business transactions. The use of terms commonly associated with paper transactions (e.g., ''copy'', ''document'', ''page'', ''printed'', ''sealed envelope'' and ''stamped'') shall not be interpreted to restrict the use of electronic commerce.

Electronic data interchange (EDI), as used in this subpart, means a technique for electronically transferring and string formatted information between computers utilizing established and published formats and codes, as authorized by the applicable Federal Information Processing Standards.

Implementation convention (IC), as used in this subpart, means the common practices and/or interpretations of the use of ANSI X12 standards. Conventions define how trading partners will use the standards for their mutual needs. The Federal IC will be used by organizational elements of the Federal community and by government organizations and by Trading Partners to exchange data with the Federal community.

Trading partner, as used in this subpart, means a business that has agreed to exchange business information electronically.

Transaction set, as used in this subpart, means the data that is exchanged to convey meaning between Trading Partners engaged in EC/EDI.

[60 FR 34744, July 3, 1995, as amended at 61 FR 39191, July 26, 1996]

4.502 Policy.

(a) The Federal Government shall use FACNET whenever practicable or cost-effective. Contracting officers may supplement FACNET transactions by using other media to meet the requirements of any contract action governed by the FAR (e.g., transmit hard copy of drawings).

(b) Before using FACNET, or any other method of electronic data interchange, The agency head shall ensure that the electronic data interchange